

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-244495

(43)Date of publication of application : 08.09.2000

(51)Int.Cl.

H04L 12/24

H04L 12/26

H04L 12/56

(21)Application number : 11-044134

(71)Applicant : HITACHI LTD

(22)Date of filing : 23.02.1999

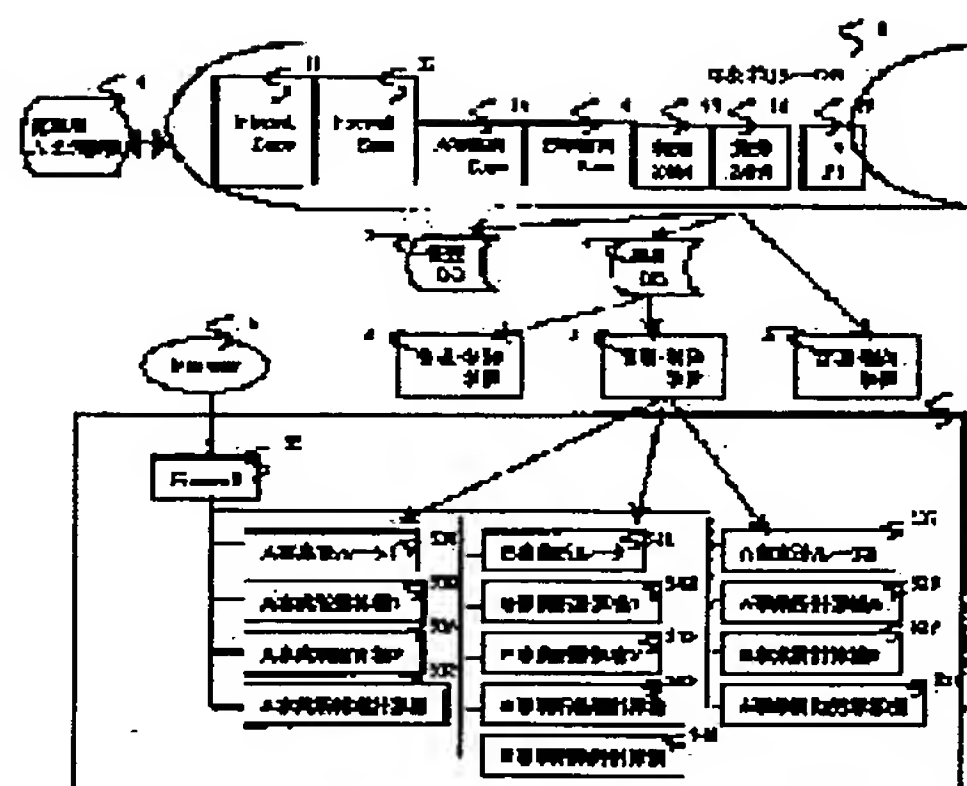
(72)Inventor : YOSHIDA KENICHI  
MIYAKE SHIGERU  
HIRATA TOSHIAKI  
KOIZUMI MINORU  
TAKADA OSAMU

## (54) NETWORK MANAGING SYSTEM

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To easily execute necessary setting by setting an operation policy stored in a data base to be the description of a job content executed in a unit constituting a network and converting the description of the job content into control information on the unit constituting the network based on an appropriate processing.

**SOLUTION:** An operation policy stored in a data base is the description of a job content executed in a unit constituting a network and the description of the job content is converted into control information on the unit constituting the network based on an appropriate processing. A company network which is formed of two offices and accounting section/industry section managing the two offices and which uses TCP/IP technology is assumed for the network 5 of a management object. Center policy DB1 stores the operation policy of the network 5 and is constructed on a general computer. A management controller 3 supports the transmission of data between center policy DB1 and the unit constituting the network 5 in the middle of them.



## LEGAL STATUS

[Date of request for examination]

17.01.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

\* NOTICES \*

Japan Patent Office is not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

---

CLAIMS

---

[Claim(s)]

[Claim 1] The network management system which the employment policy memorized by this database is description of the work breakdown performed by the device which constitutes this network, and is characterized by being changed into the control information of the device which constitutes a network based on processing with an appropriate description of this work breakdown in the network management system which consists of a database which memorizes the employment policy of the network which consists of a router, a computer, etc., and this network.

[Claim 2] The network management system characterized by having supervisory control equipment which supports both communication of information to the publication of a claim 1 in the middle of the device which constitutes this database and this network in a network management system.

[Claim 3] The network management system characterized by having the duplicate database of this database in the publication of a claim 1 in a network management system.

[Claim 4] The network management system characterized by being the business which the user group for whom description of this work breakdown uses a \*\* network takes charge of in a network management system a claim 1 or given [ any 1 ] in three.

[Claim 5] The network management system characterized by being description about the application program performed on the computer by which description of this work breakdown was connected to the \*\* network in a network management system a claim 1 or given [ any 1 ] in three.

[Claim 6] The network management system with which description about this user group's business in its duty is characterized by including the information about this user program that carries out user group use, and the information about the user group with whom this user program communicates in a network management system according to claim 4.

[Claim 7] The network management system characterized by the description about this application program including the information about the communications protocol which this application program uses, and the information about a communication place in a network management system according to claim 5.

---

[Translation done.]

★ NOTICES \*

Japan Patent Office is not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[The technical field to which invention belongs] this invention relates to the network management system and management method for offering the structure which sets up the access list, QoS setup, VPN setup, etc. of a large-scale network simply while consisting of subnetworks in which many management policies differ from two or more routers or Firewall equipment especially with respect to a computer network.

[0002]

[Description of the Prior Art] In the large-scale network while consisting of subnetworks in which many management policies differ from two or more routers or Firewall equipment conventionally, the content of a setting of each router or Firewall equipment was remarkable, and it was complicated. For example, RFC2401 etc. took the technical force advanced for understanding these to security-related technology, such as VPN (Virtual Private Network), although, as for QoS (Quality of Service)-related technology, specification was described by RFC2205 etc. Moreover, in relation to these specification, the method of distributing a setup automatically from a remote place point is also devised (for example, draft-ietf-rap-cops-05.txt of Internet Draft etc.). However, it is the same at the point of needing network instrument setup knowledge.

[0003]

[Problem(s) to be Solved by the Invention] For this reason, an important setup or an important setup of QoS were not fully released in the conventional network administration on security like the insufficient shell access list of experts with an advanced know how, or VPN, this invention solves the above-mentioned technical problem, and aims at offering the network management system which can perform a required setup simple, and a management method. Moreover, it aims at offering the software used for each computer which realizes the above-mentioned managerial system and a management method.

[0004]

[Means for Solving the Problem] In order to attain the above-mentioned purpose, this invention offers the structure which generates automatically and sets up a setup of each router, Firewall equipment, etc. from the definition about the business performed on a network. This structure enables it to perform complicated network administration simply by the conventional method. Namely, in addition to an expert like an access list or VPN, a required setup can be performed now simple by changing a difficult setup of a setup from a work breakdown intelligible for a user automatically.

[0005]

[Embodiments of the Invention] Hereafter, one example of this invention is explained in detail. Drawing 1 is drawing having shown the example of composition of the network which applied this invention. In drawing 1, 5 is a network for management and assumes the network in a company using the TCP/IP technology which consists of an accounting department and a labor division which manages two places of business and both places of business here. 1 is the central policy DB which memorizes the employment policy of a network 5, and is the database built on the

common computer, 11, 12, 13, 14, 15, 16, and 17 are the examples of the content of storage of the central policy DB1, and 11-16 are what described the example of operating which the user group using a network 5 takes charge of, and show the example of a content to drawing 2. 17 is description about the application program performed on the computer connected to the network 5, and shows the example of a content to drawing 3. 2 is the duplicate DB which copied the content of the central policy DB1, and is good in the suitable database on a computer. 3 is supervisory control equipment which supports both communication of information in the middle of the device which constitutes the central policy DB1 and a network 5, and is good by the common computer possessing the suitable program. 4 is an administrative I/O device for displaying and correcting the content of the central policy DB1, and is good at the I/O device of a suitable computer.

[0006] A network 5 is constituted from a computer 532, 533, 535, 536, 538, 539, 542, 543, 545, 546 and a router 531, 541, and 537 by drawing 1, and it connects with Internet 6 through the fire wall 52. Among these, a router 531 and 537 A computer 532, 533, 535, 536, 538, and 539 are the routers and computers of A place of business, and are a router 541. A computer 542, 543, 545, and 546 are the routers and computers of B place of business. Moreover, a computer 535 and 545 belong also to the accounting department, and a computer 536 and 546 belong also to the labor division.

[0007] Becoming important when managing intranet like a network 5 sets up a fire wall 52 correctly, and it is [ that a crack is only made not to be carried out and ] from the outside. The work breakdown of an accounting department or a labor division has much information to which secret nature should be kept in in the company. Moreover, there may be information mutually made secret also between places of business. In such a case, it is necessary to set up a network device so that the access control by VPN or the router may be performed and unnecessary information transfer may not be performed. moreover, business -- extensive and high-speed communication quality is needed depending on an application, and QoS control should be performed With the conventional technology, the manager of a network 5 needed to set up the access list and VPN of a router 531, 541, and 537 grades so that the above-mentioned demand might be filled. However, a setup of VPN or QoS was complicated, and when sufficient setup was not made from shortage of an expert, there was. Below by this invention, the demand from the above business explains that it can generate automatically to network instrument setup information, such as a router.

[0008] Drawing 2 is the example of a content of the Zone definition memorized by the central policy DB. By this example, Zone means the user group using a network. Description concerning [ the Zone definition illustrated by drawing 2 ] this user group's business in their duty is the information about this user program that carries out user group use, and the information about the user group with whom this user program communicates. The example of a content of drawing 2 is specifically an example of description for every operating group about the application program performed on the computer which was memorized by the central policy DB1, and which was connected to the network 5. The definition of the application program by which 111 are performed in Internet relation among drawing 2, The definition of the application program by which 121 is performed in Firewall relation, The definition of the application program by which 131 is performed in A place-of-business relation, The definition of the application program by which 141 is performed in B place-of-business relation, The definition of the application program by which 151 is performed in accounting relation, and 161 are the definitions of the application program performed in labor relation, and the name and communication place of a user program are specified, respectively.

[0009] By Internet Zone, as for drawing 2 and 111, Electrons mail (111), news (1112), and WWW (1113) and telnet (1114) communicate between Firewall Zone as an application program, among these, as for Electron mail, what communication is preferentially processed for (inside of 1111 and a priority) is specified. Moreover, what (1114) telnet forbids communications processing other than Firewall for clearly is specified. This specification is changed into a setup of prohibition of explicit access in a router by the below-mentioned algorithm. The line (1115) of the further 111 last specifies that applications other than the above communicate with Internet

Zone. as for drawing 2 and 121, news(1212)/telnet (1215) communicates among all Zone(s) by Electron mail communicating in all Zone(s) and priorities as an application program in FireWall Zone (1211), and WWW communicates only between Internet Zone -- having (1213) -- WWW proxy specifies what is communicated between A and B place of business (1214) [0010] Drawing 2 and 131 specify what (1314) Electrons mail (1311), news (1312), and WWW proxy (1313) communicate with Firewall Zone, and telnet communicates with FireWall Zone and B place of business, and the thing which the user program which uses port numbers 4096 and 4097 communicates between B places of business (1315 and 1316) in A place of business. Moreover, Telnet, the port number 4096, and the user program that uses 4097 are clearly forbidden from performing communication with Internet Zone. Moreover, it specifies carrying out data communication of the user program of a port number 4096 preferentially in priority size (1314, 1315, and 1316).

[0011] Although drawing 2 and 141 are the definitions of B place of business and are the same as that of the definition of A place of business, about telnet, use between FireWall Zone is also forbidden only between A places of business (1414). drawing 2 and 151 -- an accounting-related definition -- accounting-related business -- electrons mail (1511), WWW proxy (1512), and telnet (1513) the user program of port numbers 5001-5003 -- it is (1514, 1515, and 1516) -- it is only communication inside accounting Zone and communication with its other post is forbidden Drawing 2 and 161 are the definitions for the labor related operating groups which restricted communication to Labor Zone similarly.

[0012] Drawing 3 is the example of a definition of the information about the communications protocol which the application program memorized by the central policy DB uses, and the information about a communication place, and calls AP definition below. Drawing 3 and 171 are definitions independent [ user-program AP1 ]. AP1 is performed from the program AP 171 performed by the computer of the A place of business Zone, and two subprograms of AP172 of A place of business performed only especially by the computer 2. Moreover, that AP171 communicates by the computer 1 and port number 1111 of B place of business by the computer 2 and port number 1112 of (1711) and B place of business (1712), that AP172 communicates by the computer 2 and port number 1113 of B place of business by the computer 1 and port number 1114 of (1713) and B place of business (1714), and communicating by arbitrary computers and port numbers 1115 of A place of business (1715) are specified.

[0013] Drawing 2 and the content of storage of the central policy DB1 explained using 3 are the examples which summarized a setup of communication required for the business performed in a company, and a setup of the ban on communication for security maintenance by the tabular format above. Drawing 2 is an example of a definition about the business of the place of business which is an organization in a company, and drawing 3 is an example of a definition about the application program used in a company.

[0014] The network administration by this invention sets up automatically the equipment which constitutes a network based on the above information. At this time, it is also possible to express the above information graphically to administrative I/O device 4 etc. Drawing 4 is the graphical example of a display of the Zone definition corresponding to drawing 2. Drawing 5 is the example of a display of AP definition corresponding to drawing 3. Moreover, drawing 6 is the example of a display of only the information on telnet (114, 1215, 1314, 1414, 1513, 1513, and 1613) among the information on drawing 2 . Notice these about it being the content same as information about the management policy of a network. For example, if drawing 4 changes a line type and the information on the communication place for every application classification is displayed as a line after it displays the box corresponding to Zone on the suitable position on a screen, it is generable from drawing 2. At this time, if the information on the ban on communication puts x mark on a line, it can be displayed. When the drawing which added the information on the ban on communication to drawing 4 is considered, conversion to drawing 2 is also easy.

[0015] The manager who manages a network by this invention is correcting the content of the central policy DB1 through administrative I/O device 4, and manages a network. In this case, the content of the central policy DB1 may be corrected by correcting the information on drawing 2 and a tabular format like 3, and drawing 4 and a graphical display like 5 and 6 may be corrected

using the editor ability for figures.

[0016] Drawing 7 is the example of a definition of the supplementary information memorized by the central policy DB1. In the managerial system of the network by this invention, the physical configuration information of a network 5 other than the employment policy of a network is memorized of the central policy DB1. Drawing 7 and 100 are the examples of a router definition, and 101 is the example of a VPN definition. To drawing 7 and 100, the router (1001) of a name called router1 FireWall Zone and IP address 192.100.1, it is connected with the interface of a subnet mask 255.255.0.0 (1003). A place of business and IP address 192.11.0.1, it is connected with the interface of a subnet mask 255.255.0.0 (1004). B place of business and IP address 192.12.0.1, it is connected with the interface of a subnet mask 255.255.0.0 (1005). It is IP address 192.13.0.1 to another site (for example, office in the place locally left although it was the place of business same on a company organization) of A place of business. What is connected with the interface of a subnet mask 255.255.0.0 (1006) is described. Moreover, memorizing the initial setting file of router generated using drawing 2 and 3 or 7 information to a file called X1 is specified (1002).

[0017] It specifies that drawing 7 and 101 use the virtual network (VPN: Virtual Private Network) technology in which encryption communication and authentication technology were used for security reservation in order to carry out accounting business. The name of this virtual network is specifically VPN1 (1011). The IP addresses of the machine which participates are 192.11.0.10 (equivalent to A place-of-business accounting computer 535 at drawing 1), and 192.12.0.10 (equivalent to B place-of-business accounting computer 545 at drawing 1) (1012). The initial-setting files generated to each machines are X192.11.0.10 and X192.12.10.10, respectively (1013). In order to send using Y1 as a cipher system (1014), using Y2 as an authentication method (1015), and required data, it specifies using a port number 5000 (1016).

[0018] Drawing 8 and 302 are drawing 2 and the setting information for interface 1 of router1 made from 3 or 7 information. The interface address and the information (3021) on a subnetwork are created from the information (1004) on drawing 7 by drawing 8. The information on the access permission and disapproval not more than it is generated from drawing 2 and the information on 3. (The creation method is later mentioned using drawing 12) . A setup (3022) to which communication with 192.13.0.0/255.255.0.0 is permitted about all the port numbers to begin means permitting all communications from another location of the same place of business. The access permissions (3023) of the following port numbers 1111-1114 are drawing 3 and a setup corresponding to 171. A setup (3024) of the following port numbers 23 (telnet)-4097 is a setup corresponding to drawing 2 and the ban on communication of 131. A setup (3025) of the following port number 5000 is a setup corresponding to drawing 7 and a VPN setup of 101. A setup (3026) of the following port numbers 25-23 is a setup corresponding to the communication specification with FireWall Zone of drawing 2, the electrons mail (25) and news of 131 (119), WWW proxy (8080), and telnet (23). The following port numbers 23-4097 are setup (3027) corresponding to the communication specification with drawing 2 and B place of business of 131.

[0019] Drawing 8 and the last access disapproval (3028) are setup for not permitting communication except the above setup. As for the example of setting information illustrated to drawing 8, the information on the access permission and disapproval of a router assumes that actual access is controlled by specification of the permission and the disapproval of access that check in order and conditions were fulfilled first. Since the information on 302 is checked sequentially from a top, specification of the last access disapproval becomes the meaning of disapproval altogether except the above-mentioned setup.

[0020] The information on a priority is changed from the information on drawing 2 and the priority of 3 by drawing 8. The structure of QoS changes with use of the hardware of a router. Drawing 2 and the priority of 3 are specification of a due to occupational cases priority, and the information on the priority of drawing 8 is specification of the changed priority that the structure of QoS which a router hardware supports was followed. In the case of this example, it assumes transposing specification of size, inside, and smallness to priority simply. Drawing 8 and 303 are the setting information on VPN made from drawing 2, the information on 151, and drawing 7 and

the information on 101. VPN-related setting information is information from drawing 7, and the information on an access permission is drawing 2 and information from 151.

[0021] Conventionally, after he was conscious of drawing 2 and the employment policy of the network illustrated to 3, the operational administration person of a network had set up manually a setup of the router illustrated to drawing 8, and VPN. However, the know how was needed for such a setup and it was not able to do simply. Moreover, according to the work breakdown, the way of thinking of describing an employment policy was not common, either, drawing 2 and the database itself illustrated to 3 were not maintained on the computer, and the attempt of automatic creation of a setup illustrated to drawing 8 was not successful. In this example, the algorithm later mentioned using drawing 12 generates the information on drawing 8 from drawing 2 and 3 or 7 information.

[0022] It is the database formed in order for duplicate DB2 to distribute the load of the central policy DB1 in a large-scale network configuration in this example. In the management policy of a network, it refers to the real time, and a problem may arise in the response time etc. in the usual database system. Management and a control unit 3 are equipment formed for the purpose, such as improvement in the response time, and has the information which changed into a setup (it illustrates to drawing 8) of a router (it illustrates to drawing 2 and 3) the content memorized of the central policy DB, and the information for change of setting information in supervisory control equipment 3 in this example for the improvement in a speed of response. You may perform conversion to the information illustrated from drawing 2 and the information illustrated to 3 and 7 to drawing 8 by the central policy DB1. Moreover, you may carry out by duplicate DB2 and management and a control unit 3 may perform. Hereafter, suppose that it changes with supervisory control equipment 3 in this example.

[0023] The information on drawing 8 generated in this example assumes the configuration file only once [ of the start ] to set it as a network device manually. Setting change of the 2nd henceforth is automatable. The example of the content of storage which is memorized to supervisory control equipment 3 at drawing 9 for the reason is shown. 300 is the example of the data for router control of the supervisory control equipment 3 interior in drawing 9, and 301 is the example of the data for VPN control of the supervisory control equipment 3 interior. Drawing 9 and the content of storage illustrated to 300 are the interface information (3003, 3004, 3005, and 3006) and the control-system (3007) authentication methods (3008) of a router required in order to set router1 as 2nd henceforth from the outside. When using this information and drawing 2 and the content of 3 and 7 are changed, the supervisory control equipment 3 which received the changed content of drawing 8 can change a setup of the interface safely specified by encryption communication, after attesting to a router according to the specified authentication method. Specifically, the object with the same information on drawing 9 is manually set as network devices, such as a router, with the information on drawing 8 only once [ of the start ]. Since the information about the control / authentication method with same supervisory control equipment 3, router, etc. is sharable by this, supervisory control equipment 3 makes control / setting change of the router etc. via a network. Drawing 9 and 301 are the examples of information which supervisory control equipment should have in VPN setting change similarly.

[0024] Drawing 10 is the example of the data communication protocol used between the central policy DB1, duplicate DB2, and management and a control unit 3. The arbitrary protocols suitable for the duplicate of a database should just be used between the central policy DB1 and duplicate DB2. Between management and a control unit, and a router, when there is a limit on mounting of a router, use of a simple protocol like SNMP, the protocol suitable for renewal of dynamic like COPS, and a protocol like LDAP can be considered. A protocol like HTTP can also be used between the central policy DB1, or duplicate DB2, and management and a control unit 3. [0025] Drawing 11 is an example of data flow in case supervisory control equipment 3 generates setting information. What is necessary is just to merge a result independently finally in this example, respectively, although automatic generation is considered for a setup of the interface information on a router (72), an access list (73), QoS (74), and VPN (75) (76). Drawing 8 and 302 have brought a result which merged interface information and the information on an access

control.

[0026] Drawing 12 is an example of an algorithm in case supervisory control equipment 3 generates the setting information on an access permission and disapproval relation in the processing 73 of the algorithm illustrated to drawing 11. Hereafter, operation of drawing 12 is explained to an example for the generation process of an access related setup illustrated to drawing 8. In drawing 12, an access related setup of drawing 8 is generated in order of the lower shell. For this reason, the access disapproval definition of all services (port number) is first defined as a content of an access control list (81). Thereby, a setup (3028) of drawing 8 and the last access disapproval is generable. Next, the existence of the service whose access permission has been processed is investigated in drawing 2, and a permission setup of access to (82) and its service is generated (83). A setup (3026) of the port numbers 25-23 corresponding to a setup (3027) of the port numbers 23-4096 corresponding to the communication specification with drawing 2, telnet (23) of 131, 4096, and B place of business of 4097, and drawing 2 on it, the electrons mail (25), news (119), and WWW proxy of 131 (8080) and the communication specification with Firewall Zone of telnet (23) is generated by this processing. The access permission (3025) of the port of No. 5000 is also outputted here. This is generated by searching the information on the port number which VPN uses, and the computer which has participated to the VPN from drawing 7 and the information on 101.

[0027] Next, the existence of the service whose access disapproval has been processed is investigated in drawing 2, and a disapproval setup of access to (84) and its service is generated (85). A setup (3024) of drawing 2 and the access disapproval of the port numbers 23 (telnet)-4097 corresponding to the ban on communication of 131 is generated by this processing. next, the processed business of access information -- (87) which investigates the existence of an application and adds the definition of the access permission to (86) and its business AP to the head of an access list A setup (3023) of the access permission of drawing 3 and the port numbers 1111-1114 corresponding to 171 is generated by this processing. From another location of the same place of business, all communications are permitted at the end (88). A setup (3022) of communication permission with 192.13.0.0/255.255.0.0 is generated about all port numbers by this processing.

[0028] The information on the priority of drawing 8 is convertible from the information on drawing 2 and the priority of 3 in process of the above. Although the structure of QoS changes with use of the hardware of a router as mentioned above, if it carries out easy [ of the correspondence table for changing specification of drawing 2 and the priority of 3 into the information on the priority of drawing 8 ], when generating an access list in process of the above, the information on a priority can also be changed simultaneously. The central policy DB1 and duplicate DB2 are good in the suitable database constituted on a common computer. Moreover, supervisory control equipment 3 is also good by the common computer possessing the suitable soft ware. The example of composition of the computer which fitted drawing 13 at these is shown. The computer 900 illustrated to drawing 13 is the thing of general composition, and consists of main storage 901, a central processing unit 902, a network control unit 903, a display controller 905, a disk controller 907, and a disk unit 906. What is necessary is just to connect display 8 and Local Area Network 904 to a computer 900 as an external device.

[0029] When using this computer 900 as a computer which builds the central policy DB1 or duplicate DB2 on it, drawing 2 and the data illustrated to 3 and 7 are memorized by the database on a disk unit 906. This database is controlled by the suitable database software which is memorized on main storage 901 and processed with a central processing unit 902. Moreover, when using this computer 900 as supervisory control equipment 3, drawing 8 and the data illustrated to 9 are memorized by the database on a disk unit 906. This database is controlled by the suitable database software which is memorized on main storage 901 and processed with a central processing unit 902. Moreover, drawing 11 and processing illustrated to 12 are performed with the suitable software which is memorized on main storage 901 and processed with a central processing unit 902.

[0030] In the above example, the example of a definition about the business of the place of business which is an organization in a company, and the example of a definition about the

application program used in a company were memorized of the central policy DB1. Both these may be memorized of the central policy DB1, and either may be memorized of it. Moreover, although the physical configuration information of a network was memorized together of the same central policy DB1, what is memorized in another database is sufficient. The content of storage of the central policy DB1 may be corrected by correcting the information on drawing 2 and a tabular format like 3, and may correct drawing 4 and a graphical display like 5 and 6 using the editor ability for figures. A storage gestalt may also be memorized by the tabular format and you may memorize diagrammatically. Moreover, an immediate memory may be carried out to the file of a computer, and it does not matter even if it memorizes using a relational database, a directory server, etc.

[0031] Conversion to drawing 2 and the information illustrated from the information illustrated to 3 and 7 to drawing 8 which illustrated the algorithm by drawing 11 and 12 may be performed by the central policy DB1, and may be performed by duplicate DB2. Moreover, management and a control unit 3 may perform. A database may be constituted only from a central policy DB1, and may consist of a central policy DB1 and duplicate DB2. The function of supervisory control equipment may be executed by proxy with the central policy DB or Duplicate DB, and supervisory control equipment may be omitted. The information generated from information, such as drawing 2, and 3, 7, may also include arbitrary setup about router control, and may reduce a labor in arbitrary setup. For example, a setup of QoS may be generated, and as long as it is unnecessary, you may omit it. As a candidate of the item set up, an access list, a path control method, an authentication method, a cipher system, QoS, etc. can be considered.

[0032] Moreover, although the method of introducing software and constituting this invention from drawing 13 to a common computer was illustrated, the computer beforehand equipped with ROM which wrote in exclusive software may be used, or what hardware-ized the required portion may be used. In addition, the above-mentioned software by which introduction is carried out is introduced into each computer through magnetic-recording media, such as FD and CD-ROM, an optical recording medium, or the network connected to other servers.

[0033]

[Effect of the Invention] The security and the QoS function of a network can be improved by offering the structure which sets up the access list, QoS setup, VPN setup, etc. of a large-scale network simply while consisting of subnetworks in which many management policies differ from two or more routers or Firewall equipment in the above example according to this invention so that clearly, and setting up a network device correctly.

.....  
[Translation done.]

## \* NOTICES \*

Japan Patent Office is not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

---

DESCRIPTION OF DRAWINGS

---

## [Brief Description of the Drawings]

[Drawing 1] The example of composition of the network by this invention.

[Drawing 2] Example of a content of the central policy DB1 (Zone definition) .

[Drawing 3] Example of a content of the central policy DB1 (AP definition) .

[Drawing 4] The example of a content display of the central policy DB1 corresponding to the definition illustrated by drawing 2.

[Drawing 5] The example of a content display of the central policy DB1 corresponding to the definition illustrated by drawing 3.

[Drawing 6] The example of the content display classified by application of the central policy DB1.

[Drawing 7] The example of a definition of supplementary information.

[Drawing 8] The generated example of configuration information.

[Drawing 9] The example of the content of storage of supervisory control equipment 3.

[Drawing 10] The example of a data communication protocol.

[Drawing 11] The example of data flow of a configuration information generate time.

[Drawing 12] The example of an algorithm for configuration information generation.

[Drawing 13] The central policy DB1, duplicate DB2, and the example of composition of supervisory control equipment 3.

## [Description of Notations]

1 [ — Supervisory control equipment, 4 / — Administrative I/O device, ] — The central policy DB, 2 — Duplicate DB, 3 5 [ — The content of storage of the central policy DB, ] — Intranet, 6 — The Internet, 11, 12, 13, 14, 15, 16, 17 100 — The example of the router definition inside central policy DB, 101 — The example of the VPN definition inside central policy DB, 111 — The Internet Zone definition inside central policy DB, 121 — The FireWall Zone definition inside central policy DB, 131 [ Zone definition, ] — The A place-of-business Zone definition inside central policy DB, 141 — B place of business inside central policy DB 151 — The accounting Zone definition inside central policy DB, 161 — The labor Zone definition inside central policy DB, the application inside 171 — central policy DB — the definition of AP1, and the example of the data for router control inside 300 — supervisory control equipment — 301 — The example of the data for VPN control inside supervisory control equipment, 302 — The example of a router setup inside supervisory control equipment, 303 — The example of a VPN setup inside supervisory control equipment, 52 — Fire wall, 531,541,537 [ — The computer of the B place of business Zone, 535,545 / — The computer of Accounting Zone, 536,546 / — Computer of Labor Zone. ] — A router, 532, 533, 535,538,539,536 — The computer of the A place of business Zone, 542,543,545,546

---

[Translation done.]

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号  
特開2000-244495  
(P2000-244495A)

(43)公開日 平成12年9月8日(2000.9.8)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード(参考)
H 0 4 L 12/24		H 0 4 L 11/08	5 K 0 3 0
12/26		11/20	1 0 2 A 9 A 0 0 1
12/56			

審査請求 未請求 請求項の数7 O L (全 15 頁)

(21)出願番号 特願平11-44134

(22)出願日 平成11年2月23日(1999.2.23)

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 吉田 健一

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72)発明者 三宅 滋

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(74)代理人 100068504

弁理士 小川 勝男

最終頁に続く

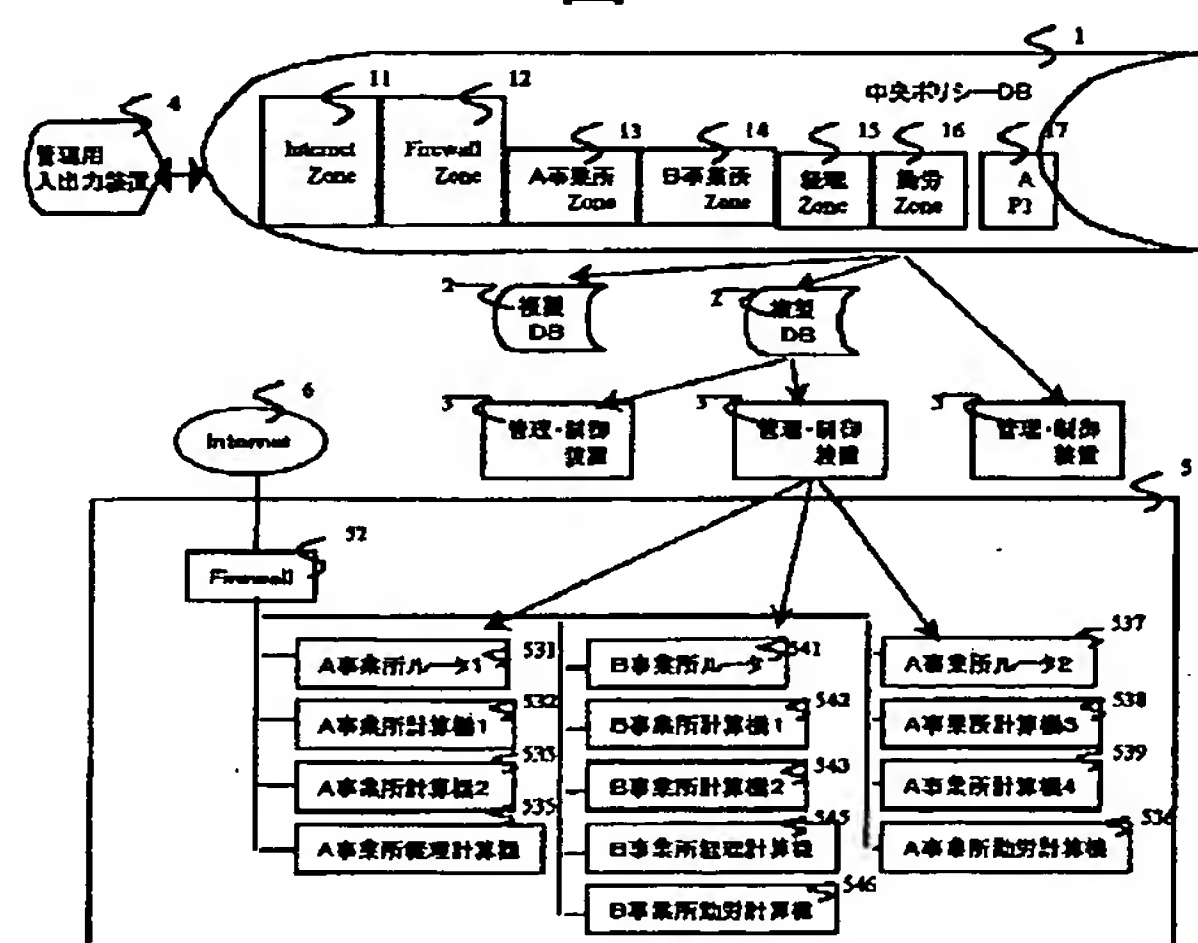
(54)【発明の名称】 ネットワーク管理システム

(57)【要約】

【課題】複数のルータやFirewall装置と、多数の管理ポリシーの異なるサブネットから構成される中・大規模のネットワークでは、個々のルータやFirewall装置の設定内容が複雑となるため、高度な技術力が必要とされる。しかし専門家の不足からアクセスリストやVPNのようなセキュリティ上重要な設定やQoSの設定は、従来は十分になされていなかった。

【解決手段】ネットワーク上の計算機でプログラムにより実行される業務内容の定義から、個々のルータやFirewall装置などの設定を自動生成・設定する仕組みを実現し、ネットワーク管理を単純に行う仕組みを提供する。ネットワーク機器が正しく設定されることにより、ネットワークのセキュリティやQoS機能が向上する。

図1



## 【特許請求の範囲】

【請求項1】 ルータや計算機などから構成されるネットワークと、該ネットワークの運用ポリシーを記憶するデータベースよりなるネットワーク管理システムにおいて、

該データベースに記憶される運用ポリシーが、該ネットワークを構成する機器で実行される業務内容の記述であり、該業務内容の記述が適当な処理に基づきネットワークを構成する機器の制御情報に変換されることを特徴とするネットワーク管理システム。

【請求項2】 請求項1の記載にネットワーク管理システムにおいて、

該データベースと該ネットワークを構成する機器の間で両者の情報伝達をサポートする管理制御装置を持つことを特徴とするネットワーク管理システム。

【請求項3】 請求項1の記載にネットワーク管理システムにおいて、

該データベースの複製データベースを持つことを特徴とするネットワーク管理システム。

【請求項4】 請求項1ないし3いずれかに記載のネットワーク管理システムにおいて、

該業務内容の記述が概ネットワークを利用するユーザーグループの担当する業務であることを特徴とするネットワーク管理システム。

【請求項5】 請求項1ないし3いずれかに記載のネットワーク管理システムにおいて、

該業務内容の記述が概ネットワークに接続された計算機の上で実行されるアプリケーションプログラムに関する記述であることを特徴とするネットワーク管理システム。

【請求項6】 請求項4に記載のネットワーク管理システムにおいて、

該ユーザーグループの担当業務に関する記述が、該ユーザーグループ使用する業務プログラムに関する情報と、該業務プログラムが通信を行うユーザーグループに関する情報を含むことを特徴とするネットワーク管理システム。

【請求項7】 請求項5に記載のネットワーク管理システムにおいて、

該アプリケーションプログラムに関する記述が、該アプリケーションプログラムの使用する通信プロトコルに関する情報と通信先に関する情報を含むことを特徴とするネットワーク管理システム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は計算機ネットワークに係わり、特に複数のルータやFirewall装置と、多数の管理ポリシーの異なるサブネットから構成される中・大規模のネットワークのアクセスリスト・QoS設定・VPN設定などの設定を簡単に行う仕組みを提供するためのネッ

トワーク管理システムおよび管理方式に関する。

## 【0002】

【従来の技術】 従来、複数のルータやFirewall装置と、多数の管理ポリシーの異なるサブネットから構成される中・大規模のネットワークにおいては、個々のルータやFirewall装置の設定内容が著しく複雑となっていた。例えば、VPN(Virtual Private Network)などセキュリティ関係の技術はRFC2401などに、QoS(Quality of Service)関連の技術はRFC2205などに規格が記述されているが、これらを理解するには高度な技術力を要した。また、これら規格に関連して、遠隔地点から設定を自動配布する方法も考案されている（例えばInternet Draftのdraft-ietf-rap-cops-05.txt等）。しかしながら、ネットワーク機器の設定知識を必要とするという点では同じである。

## 【0003】

【発明が解決しようとする課題】 この為、高度な専門知識を持つ専門家の不足からアクセスリストやVPNのようなセキュリティ上重要な設定やQoSの設定は、従来のネットワーク管理においては十分にはなされていなかった。本発明は、上記課題を解決し、必要な設定を簡便に行なえるネットワーク管理システム、管理方法を提供することを目的とする。また、上記管理システム、管理方法を実現する、個々の計算機に用いるソフトウェアを提供することを目的とする。

## 【0004】

【課題を解決するための手段】 上記目的を達成するために、本発明は、ネットワーク上で実行される業務に関する定義から、個々のルータやFirewall装置などの設定を自動生成・設定する仕組みを提供する。この仕組みによって、従来方法では複雑であったネットワーク管理を単純に行うことが可能になる。すなわち、アクセスリストやVPNのような専門家以外には設定の難しい設定を、利用者にわかりやすい業務内容から自動変換することで、必要な設定が簡便に行なえるようになる。

## 【0005】

【発明の実施の形態】 以下、本発明の一実施例を詳細に説明する。図1は本発明を適用したネットワークの構成例を示した図である。図1において、5は管理対象のネットワークであり、ここでは2つの事業所と、両方の事業所の管理を行う経理課・勤労課からなるTCP/IP技術を用いた企業内ネットワークを想定している。1はネットワーク5の運用ポリシーを記憶する中央ポリシーDBであり、一般的な計算機上に構築したデータベースである。11, 12, 13, 14, 15, 16, 17は中央ポリシーDB1の記憶内容例であり、11~16はネットワーク5を利用するユーザーグループの担当する業務例を記述したもので、内容例を図2に示す。17はネットワーク5に接続された計算機の上で実行されるアプリケーションプログラムに関する記述であり、内容例を図3に示す。2は中央ポリシーDB1の内容

をコピーした複製DBであり、計算機上の適当なデータベースで良い。3は中央ポリシーDBとネットワーク5を構成する機器の中間で両者の情報伝達をサポートする管理制御装置であり、適当なプログラムを具備した一般的な計算機で良い。4は中央ポリシーDBの内容を表示・修正するための管理用入出力装置であり、適当な計算機の入出力装置で良い。

【0006】図1でネットワーク5は計算機532, 533, 535, 536, 538, 539, 542, 543, 545, 546およびルータ531, 541, 537から構成され、ファイヤーウォール52を通してInternet 6に接続されている。このうちルータ531, 537 計算機532, 533, 535, 536, 538, 539はA事業所のルータと計算機であり、ルータ541 計算機542, 543, 545, 546はB事業所のルータと計算機である。また、計算機535, 545は経理課にも、計算機536, 546は勤労課にも所属している。

【0007】ネットワーク5のようなイントラネットを管理する時に重要になるのは、ファイヤーウォール52を正しく設定し、外部からクラックされないようにするだけではない。経理課や勤労課の業務内容は社内的にも秘密性が保たれるべき情報が多い。また事業所間でも互いに秘密にしておく情報がある場合もある。このような場合、VPNやルータによるアクセス制御を行い、不必要な情報転送が行われない様にネットワーク機器を設定する必要がある。また業務アプリによっては大量・高速の通信品質を必要とし、QoS制御が行われるべき場合もある。従来技術ではネットワーク5の管理者がルータ531, 541, 537等のアクセスリストやVPNを上記要求をみたすように設定する必要があった。しかし、VPNやQoSの設定は複雑であり、専門家の不足から十分な設定がなされない場合もあった。以下本発明により、上記のような業務からの要求が、ルータ等ネットワーク機器の設定情報に自動生成できることを説明する。

【0008】図2は中央ポリシーDBに記憶されるZone定義の内容例である。本実施例ではZoneはネットワークを利用するユーザーグループを意味する。図2に例示されたZone定義は該ユーザーグループの担当業務に関する記述が、該ユーザーグループ使用する業務プログラムに関する情報と、該業務プログラムが通信を行うユーザーグループに関する情報である。具体的には図2の内容例は中央ポリシーDBに記憶された、ネットワーク5に接続された計算機の上で実行されるアプリケーションプログラムに関する業務グループごとの記述例であり、図2中、111はInternet関連で実行されるアプリケーションプログラムの定義、121はFireWall関連で実行されるアプリケーションプログラムの定義、131はA事業所関連で実行されるアプリケーションプログラムの定義、141はB事業所関連で実行されるアプリケーションプログラムの定義、151は経理関連で実行されるアプリケーションプログラムの定義、161は勤労関連で実行されるアプリケーション

プログラムの定義であり、それぞれ業務プログラムの名称と通信先を指定している。

【0009】図2、111はInternet Zoneではアプリケーションプログラムとして電子mail(1111), news(1112), WWW(1113), telnet(1114)がFireWall Zoneとの間で通信を行い、このうち電子mailは優先的に通信が処理される(1111、優先度中)ことが指定されている。またtelnetはFirewall以外との通信処理を明示的に禁止する(1114)ことが指定されている。この指定は後述のアルゴリズムにより、ルータにおける明示的なアクセス禁止の設定に変換される。さらに111最後の行(1115)は上記以外のアプリケーションがInternet Zoneと通信することを指定している。図2、121はFireWall Zoneではアプリケーションプログラムとして電子mailが全てのZoneと優先度中で通信し(1211)、news(1212)/telnet(1215)が全てのZoneとの間で通信し、WWWはInternet Zoneとの間だけで通信される(1213)が、WWW proxyがA,B事業所との間で通信を行う(1214)ことを指定している。

【0010】図2、131はA事業所では電子mail(1311), news(1312), WWW proxy(1313)がFirewall Zoneと通信し、telnetがFireWall ZoneおよびB事業所と通信する(1314)こと、ポート番号4096, 4097を使用する業務プログラムがB事業所との間で通信を行う(1315と1316)ことを指定している。またTelnetとポート番号4096, 4097を使用する業務プログラムがInternet Zoneと通信を行うことを明示的に禁止している。またポート番号4096の業務プログラムは優先度大で優先的にデータ通信することを指定している(1314, 1315と1316)。

【0011】図2、141はB事業所の定義で、A事業所の定義と同様であるが、telnetに関してはA事業所との間のみでFireWall Zoneとの間の利用も禁止している(1414)。図2、151は経理関連の定義で経理関係の業務は電子mail(1511), WWW proxy(1512), telnet(1513), ポート番号5001~5003の業務プログラムである(1514, 1515と1516)が、経理Zone内部での通信のみで、それ以外の部署との通信を禁止している。図2、161は同様に勤労Zoneのみに通信を制限した勤労関連業務グループ用の定義である。

【0012】図3は中央ポリシーDBに記憶されるアプリケーションプログラムの使用する通信プロトコルに関する情報と通信先に関する情報の定義例であり、以下AP定義と称する。図3、171は業務プログラムAPI単独の定義である。APIはA事業所Zoneの計算機で実行されるプログラムAPI171とA事業所の特に計算機2のみで実行されるAPI172の2つのサブプログラムより実行される。またAPI171はB事業所の計算機1とポート番号1111で(1711)、B事業所の計算機2とポート番号1112で(1712)通信を行うこと、API172はB事業所の計算機2とポート番号1113で(1713)、B事業所の計算機1とポート番号1114で(1714)通信を行うこと、A事業所の任意の計算機とポート番号1115で通信

を行うこと(1715)が指定されている。

【0013】以上図2、3を用いて説明してきた中央ポリシーDB1の記憶内容は、企業内で行われる業務に必要な通信の設定と、セキュリティ保持の為に通信禁止の設定を表形式でまとめた例である。図2は会社内の組織である事業所の業務に関する定義例であり、図3は会社内で使用されるアプリケーションプログラムに関する定義例である。

【0014】本発明によるネットワーク管理は、以上の情報を元に、ネットワークを構成する機器類の設定を自動的に行う。この時、以上の情報を管理用入出力装置4などにグラフィカルに表現する事も可能である。図4は図2に対応したZone定義のグラフィカルな表示例である。図5は図3に対応したAP定義の表示例である。また図6は図2の情報のうちtelnetの情報(1114、1215、1314、1414、1513、1513と1613)のみの表示例である。これらはネットワークの管理ポリシーに関する情報としては同じ内容であることに注意されたい。例えば図4は、Zoneに対応する箱を画面上の適当な位置に表示した後、アプリケーション種別ごとの通信先の情報を線種を変えて線として表示すれば図2から生成できる。この時、通信禁止の情報は線に×印をつけるなどすれば表示できる。図4に通信禁止の情報を付加した図面を考えた場合、図2への変換も容易である。

【0015】本発明によりネットワークを管理する管理者は、管理用入出力装置4を通して中央ポリシーDB1の内容を修正することで、ネットワークの管理を行う。この場合、図2、3のような表形式の情報を修正することで中央ポリシーDB1の内容を修正しても良いし、図4、5、6のようなグラフィカルな表示を図形用のエディタ機能を用いて修正しても良い。

【0016】図7は中央ポリシーDB1に記憶される補足情報の定義例である。本発明によるネットワークの管理システムでは中央ポリシーDB1にネットワークの運用ポリシーの他にネットワーク5の物理的な構成情報を記憶しておく。図7、100はルータ定義の例であり、101はVPN定義の例である。図7、100にはrouter1という名称のルータ(1001)は、FireWall ZoneとIPアドレス192.10.0.1、サブネットマスク255.255.0.0のインターフェースで繋がっており(1003)、A事業所とIPアドレス192.11.0.1、サブネットマスク255.255.0.0のインターフェースで繋がっており(1004)、B事業所とIPアドレス192.12.0.1、サブネットマスク255.255.0.0のインターフェースで繋がっており(1005)、A事業所の別のサイト(例えば会社組織上では同じ事業所だが地域的に離れた場所にあるオフィス)にIPアドレス192.13.0.1、サブネットマスク255.255.0.0のインターフェースで繋がっている(1006)ことが記述されている。また、図2、3、7の情報を使い生成したrouterの初期設定fileをX1というファイルに記憶する事が指定されている(1002)。

【0017】図7、101は経理業務を遂行するため、セキュリティ確保のために暗号化通信と認証技術を用いた仮想ネットワーク(VPN: Virtual Private Network)技術を使う事を指定している。具体的には、この仮想ネットワークの名称はVPN1であり(1011)、参加する機械のIPアドレスは192.11.0.10(図1でA事業所経理計算機535に相当)と192.12.0.10(図1でB事業所経理計算機545に相当)であり(1012)、それぞれの機械用に生成した初期設定ファイルが、それぞれX192.11.0.10とX192.12.10.10であること(1013)、暗号化方式としてY1を使うこと(1014)、認証方式としてY2を使うこと(1015)、また必要なデータを送るためにポート番号5000を利用すること(1016)を指定している。

【0018】図8、302は図2、3、7の情報から作られるrouter1のインターフェース1用の設定情報である。図8でインターフェースアドレスとサブネットの情報(3021)は図7の情報(1004)から作成する。それ以下のアクセス許可・不許可の情報は図2、3の情報から生成する。(作成方法は図12を用いて後述する)。始めの全てのポート番号に関して192.13.0.0/255.255.0.0との通信を許可している設定(3022)は、同じ事業所の別ロケーションからはあらゆる通信を許可する事を意味している。次のポート番号1111から1114のアクセス許可(3023)は図3、171に対応した設定である。次のポート番号23(telnet)~4097の設定(3024)は図2、131の通信禁止に対応した設定である。次のポート番号5000の設定(3025)は図7、101のVPN設定に対応した設定である。次のポート番号25~23の設定(3026)は図2、131の電子mail(25), news(119), WWW proxy(8080), telnet(23)のFireWall Zoneとの通信指定に対応した設定である。次のポート番号23~4097は図2、131のB事業所との通信指定に対応した設定(3027)である。

【0019】図8、最後のアクセス不許可(3028)は以上の設定以外の通信を許可しないための設定である。図8に例示した設定情報例はルータのアクセス許可・不許可の情報が順番にチェックされていき、最初に条件が満たされたアクセスの許可・不許可の指定により実際のアクセスが制御されることを想定している。302の情報は上から順にチェックされるので、最後のアクセス不許可の指定は、上記設定以外全て不許可の意味になる。

【0020】図8で優先度の情報は図2、3の優先度の情報から変換される。QoSの仕組みはルータのハードウェアの使用により異なる。図2、3の優先度は業務上の優先度の指定であり、図8の優先度の情報はルータハードがサポートするQoSの仕組みに従った変換された優先度の指定である。本実施例の場合、大・中・小の指定を単純に優先順位に置き換えることを想定している。図8、303は図2、151の情報と図7、101の情報から作られるVPNの設定情報である。VPN関連の設定情報は図7からの情報であり、アクセス許可の情報は図2、151からの情報であ

る。

【0021】従来、図8に例示したルータ、VPNの設定は図2、3に例示したネットワークの運用ポリシーを意識した上で、ネットワークの運用管理者が手動で設定していた。しかし、このような設定には専門知識を必要とし、簡単にはできなかった。また、業務内容に従って、運用ポリシーを記述しておくという発想も一般的ではなく、図2、3に例示したデータベース自体も計算機上にメンテナンスされておらず、図8に例示した設定の自動作成の試みは成功していなかった。本実施例では図12を用いて後述するアルゴリズムが図8の情報を図2、3、7の情報から生成する。

【0022】本実施例において複製DB2は大規模なネットワーク構成において中央ポリシーDB1の負荷を分散させるために設けたデータベースである。ネットワークの管理ポリシーの中には実時間で検索され通常のデータベース・システムでは応答時間等に問題が生じる場合がある。管理・制御装置3は、応答時間向上などの目的で設けた装置で、本実施例では応答速度向上のため、中央ポリシーDBに記憶した内容を(図2、3に例示)ルータの設定(図8に例示)に変換した情報と、設定情報の変更用の情報を管理制御装置3に持つ。図2、3、7に例示した情報から図8に例示した情報への変換は中央ポリシーDB1で行って良い。また、複製DB2で行っても良いし、管理・制御装置3で行っても良い。以下、本実施例では管理制御装置3で変換するとする。

【0023】本実施例においては生成した図8の情報は初めの一回だけ手動で設定ファイルをネットワーク機器に設定すると仮定している。2回目以降の設定変更は自動化できる。図9にそのために管理制御装置3に記憶する記憶内容の例を示す。図9で300は、管理制御装置3内部のルータ制御用データの例であり、301は管理制御装置3内部のVPN制御用データの例である。図9、300に例示した記憶内容は2回目以降にrouter1の設定を外部から行うために必要なルータのインターフェース情報(3003、3004、3005と3006)と制御方式(3007)認証方法(3008)である。この情報を用いれば、図2、3、7の内容が変更された時に、変更された図8の内容を受け取った管理制御装置3は指定された認証方法に従いルータに認証を行った後、暗号化通信により安全に指定されたインターフェースの設定を変更することができる。具体的には図9の情報は同じ物が初めの1回だけ図8の情報とともに手動でルータなどのネットワーク機器に設定される。これにより管理制御装置3とルータなどが同じ制御・認証方式に関する情報を共有できるので、管理制御装置3はルータなどをネットワーク経由で制御・設定変更できる。図9、301は同様にVPN設定変更用に管理制御装置3が持つべき情報例である。

【0024】図10は中央ポリシーDB1、複製DB2、管理・制御装置3の間で使われるデータ通信プロトコルの例で

ある。中央ポリシーDB1と複製DB2の間はデータベースの複製に適した任意のプロトコルを用いれば良い。管理・制御装置とルータの間は、ルータの実装上の制限がある場合は、SNMPのような単純なプロトコルや、COPSのような動的更新に適したプロトコル、LDAPのようなプロトコルの利用が考えられる。中央ポリシーDB1または複製DB2と管理・制御装置3の間はHTTPのようなプロトコルを使うこともできる。

【0025】図11は管理制御装置3が設定情報を生成する時のデータフロー例である。本実施例ではルータのインターフェース情報(72)、アクセスリスト(73)、QoS(74)、VPN(75)の設定を対象に、自動生成を考えるが、それぞれ独立して最後に結果をマージ(76)すれば良い。図8、302はインターフェース情報とアクセス制御の情報をマージした結果になっている。

【0026】図12は、管理制御装置3が図11に例示したアルゴリズムの処理73においてアクセス許可・不許可関連の設定情報を生成する時のアルゴリズム例である。以下、図8に例示したアクセス関連設定の生成過程を例に図12の動作を説明する。図12では図8のアクセス関連設定を下から順に生成していく。この為、始めに全てのサービス(ポート番号)のアクセス不許可定義をアクセス制御リストの内容として定義する(81)。これにより図8、最後のアクセス不許可の設定(3028)が生成できる。次に図2の中でアクセス許可の処理済みのサービスの有無を調べ(82)、そのサービスに対するアクセスの許可設定を生成する(83)。この処理により、図2、131のtelnet(23)、4096、4097のB事業所との通信指定に対応したポート番号23~4096の設定(3027)と、その上の図2、131の電子mail(25)、news(119)、WWW proxy(8080)、telnet(23)のFireWall Zoneとの通信指定に対応したポート番号25~23の設定(3026)が生成される。ポート5000番のアクセス許可(3025)もここで出力される。これはVPNが使用するポート番号と、そのVPNへ参加している計算機の情報(図7、101の情報)から検索することで生成する。

【0027】次に図2の中でアクセス不許可の処理済みのサービスの有無を調べ(84)、そのサービスに対するアクセスの不許可設定を生成する(85)。この処理により図2、131の通信禁止に対応したポート番号23(telnet)~4097のアクセス不許可の設定(3024)が生成される。次にアクセス情報の処理済み業務アプリの有無を調べ(86)、その業務APに対するアクセス許可の定義をアクセスリストの先頭に追加する(87)。この処理により図3、171に対応したポート番号1111から1114のアクセス許可の設定(3023)が生成される。最後に同じ事業所の別ロケーションからはあらゆる通信を許可する(88)。この処理により、全てのポート番号に関して192.13.0.0/255.255.0.0との通信許可の設定(3022)が生成される。

【0028】図8の優先度の情報は上記の過程で図2、3の優先度の情報から変換できる。前述のようにQoSの仕

組みはルータのハードウェアの使用により異なるが、図2, 3の優先度の指定を図8の優先度の情報に変換するための対応表を容易しておけば、上記の過程でアクセスリストを生成する時に同時に優先度の情報も変換できる。中央ポリシーDB1および複製DB2は一般的な計算機上に構成される適当なデータベースで良い。また、管理制御装置3も適当なソフトウェアを具備した一般的な計算機で良い。図13にこれらに適した計算機の構成例を示す。図13に例示した計算機900は一般的な構成のもので、主記憶装置901、中央処理装置902、ネットワーク制御装置903、表示制御装置905、ディスク制御装置907、ディスク装置906より構成される。表示装置8およびローカルエリアネットワーク904は外部装置として計算機900に接続すれば良い。

【0029】この計算機900を中央ポリシーDB1または複製DB2をその上に構築する計算機として用いる場合、図2, 3, 7に例示したデータは、ディスク装置906上のデータベースに記憶される。このデータベースは、主記憶装置901上に記憶され中央処理装置902で処理される適当なデータベースソフトにより制御される。また、この計算機900を管理制御装置3として用いる場合、図8, 9に例示したデータはディスク装置906上のデータベースに記憶される。このデータベースは、主記憶装置901上に記憶され中央処理装置902で処理される適当なデータベースソフトにより制御される。また図11, 12に例示した処理は、主記憶装置901上に記憶され中央処理装置902で処理される適当なソフトにより実行される。

【0030】以上の実施例では、中央ポリシーDB1に、会社内の組織である事業所の業務に関する定義例と会社内で使用されるアプリケーションプログラムに関する定義例を記憶していた。中央ポリシーDB1には、これら両方を記憶しておいても良いし、どちらか一方を記憶しても良い。また同じ中央ポリシーDB1にはネットワークの物理的な構成情報を一緒に記憶しておいたが、別のデータベースに記憶するのも良い。中央ポリシーDB1の記憶内容は、図2, 3のような表形式の情報を修正することで修正しても良いし、図4, 5, 6のようなグラフィカルな表示を図形用のエディタ機能を用いて修正しても良い。記憶形態も表形式で記憶しても良いし、図形で記憶しても良い。また計算機のファイルに直接記憶しても良いし、リレーショナルデータベースやディレクトリサーバなどを使って記憶してもかまわない。

【0031】図11, 12で、そのアルゴリズムを例示した、図2, 3, 7に例示した情報から図8に例示した情報への変換は、中央ポリシーDB1で行って良いし、複製DB2で行っても良い。また、管理・制御装置3で行ってもかまわない。データベースは中央ポリシーDB1だけで構成しても良いし、中央ポリシーDB1と複製DB2で構成しても良い。管理制御装置の機能を中央ポリシーDBや複製DBで代行し、管理制御装置を省略してもかまわない。図2, 3,

7などの情報から生成される情報も、ルータ制御に関する任意の設定を含んでかまわないし、任意の設定を省力してもかまわない。例えば、QoSの設定は生成しても良いし、必要なければ省略してかまわない。設定される項目の候補としてはアクセスリスト・経路制御方式・認証方式・暗号化方式・QoSなどが考えられる。

【0032】また図13では、本発明を一般の計算機に、ソフトウェアを導入して構成する方法を例示したが、専用ソフトウェアを書込んだROMを予め備えた計算機を用いたり、必要な部分をハードウェア化したものを用いてもよい。なお、上記導入されるソフトウェアは、FD、CD-ROMなどの磁気記録媒体、光記録媒体、または他のサーバに接続されたネットワークを介して、各計算機に導入されるものである。

【0033】

【発明の効果】以上の実施例で明らかなように、本発明によれば、複数のルータやFirewall装置と、多数の管理ポリシーの異なるサブネットから構成される中・大規模のネットワークのアクセスリスト・QoS設定・VPN設定などの設定を簡単に行う仕組みを提供し、ネットワーク機器が正しく設定されることにより、ネットワークのセキュリティやQoS機能が向上することができる。

【図面の簡単な説明】

【図1】本発明によるネットワークの構成例。

【図2】中央ポリシーDB1の内容例（Zone定義）。

【図3】中央ポリシーDB1の内容例（AP定義）。

【図4】図2で例示した定義に対応する中央ポリシーDB1の内容表示例。

【図5】図3で例示した定義に対応する中央ポリシーDB1の内容表示例。

【図6】中央ポリシーDB1のアプリケーション別内容表示例。

【図7】補足情報の定義例。

【図8】生成されたコンフィグレーション情報例。

【図9】管理制御装置3の記憶内容例。

【図10】データ通信プロトコルの例。

【図11】コンフィグレーション情報生成時のデータフロー例。

【図12】コンフィグレーション情報生成用のアルゴリズム例。

【図13】中央ポリシーDB1および複製DB2および管理制御装置3の構成例。

【符号の説明】

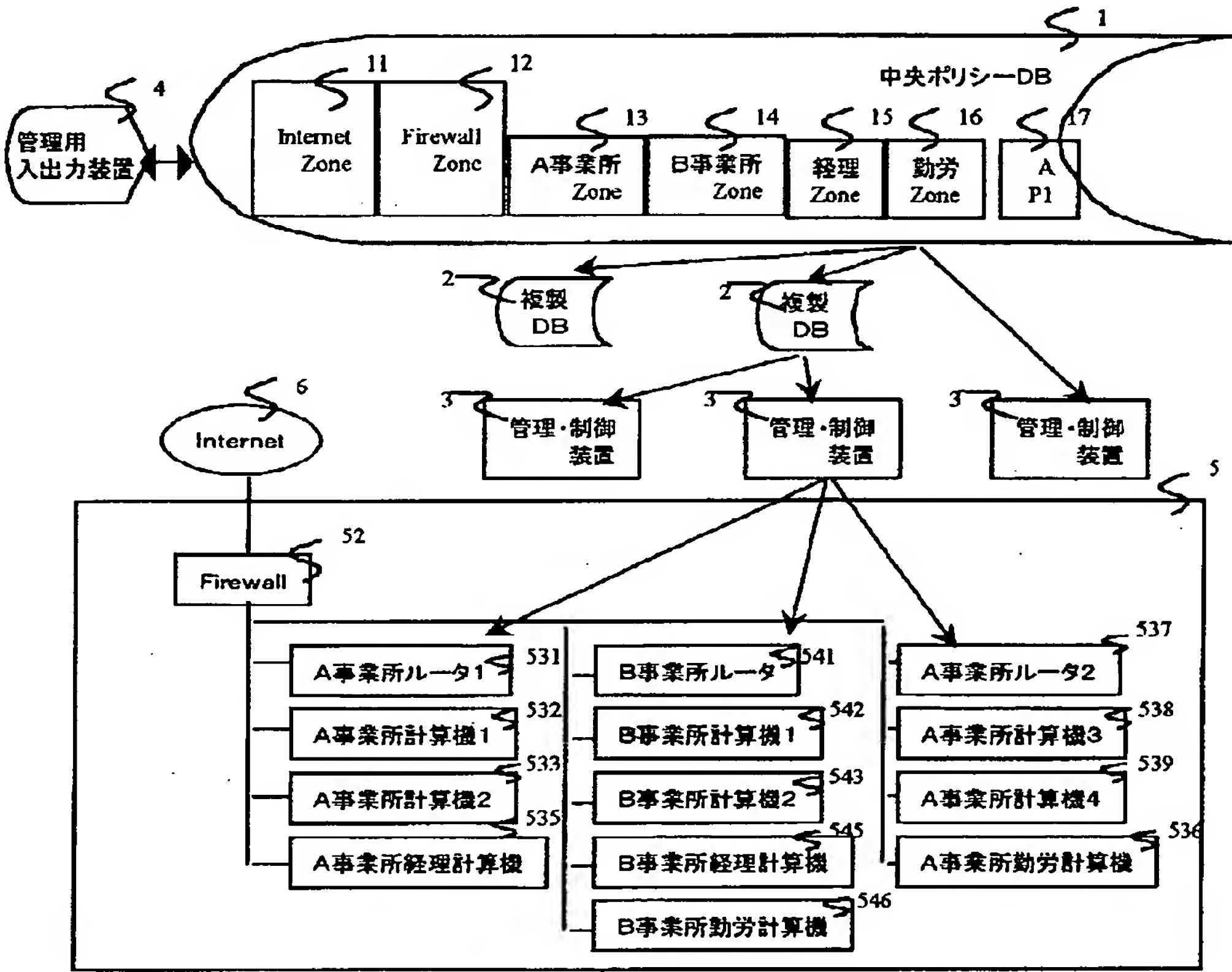
1…中央ポリシーDB、2…複製DB、3…管理制御装置、4…管理用入出力装置、5…イントラネット、6…インターネット、11, 12, 13, 14, 15, 16, 17…中央ポリシーDBの記憶内容、100…中央ポリシーDB内部のルータ定義の例、101…中央ポリシーDB内部のVPN定義の例、111…中央ポリシーDB内部のInternet Zone定義、121…中央ポリシーDB内部のFireWall Zone定義、131…中央ポリシーDB内部のA事

業所Zone定義、141…中央ポリシーDB内部のB事業所 Zone定義、151…中央ポリシーDB内部の経理Zone定義、161…中央ポリシーDB内部の勤労Zone定義、171…中央ポリシーDB内部のアプリAPIの定義、300…管理制御装置内部のルータ制御用データの例、301…管理制御装置内部のVPN制御用データの例、302…管理制御装置内部のルータ

設定の例、303…管理制御装置内部のVPN設定の例、52…ファイヤーウォール、531,541,537…ルータ、532,533,535,538,539,536…A事業所Zoneの計算機、542,543,545,546…B事業所Zoneの計算機、535,545…経理Zoneの計算機、536,546…勤労Zoneの計算機。

【図1】

図1



【図3】

図3

API定義

アプリ名	実行計算機	通信先	ポート番号	優先度
API71	A事業所Zone	B事業所計算機1	1111	中
		B事業所計算機2	1112	
API72	A事業所計算機2	B事業所計算機2	1113	
		B事業所計算機1	1114	
		A事業所Zone	1115	

【図2】

## 図2

Internet Zone定義

アプリケーション種別	通信先	優先度	通信禁止
電子mail	FireWall Zone	中	
news	FireWall Zone		
WWW	FireWall Zone		
telnet	FireWall Zone		FireWallZone以外全て
上記以外全て			全て

FireWall Zone定義

アプリケーション種別	通信先	優先度	通信禁止
電子mail	全て	中	
news	全て		
WWW	Internet Zone		
WWW proxy	A, B事業所Zone		
telnet	全て		

A事業所Zone定義

アプリケーション種別	通信先	優先度	通信禁止
電子mail	FireWall Zone	中	
news	FireWall Zone		
WWW proxy	FireWall Zone		
telnet	FireWall, B事業所Zone		Internet Zone
4096	B事業所Zone	大	Internet Zone
4097	B事業所Zone		Internet Zone

B事業所Zone定義

アプリケーション種別	通信先	優先度	通信禁止
電子mail	FireWall Zone	中	
news	FireWall Zone		
WWW proxy	FireWall Zone		
telnet	A事業所Zone		FireWall, Internet Zone
4096	A事業所Zone	大	Internet Zone
4097	A事業所Zone		Internet Zone

経理Zone定義

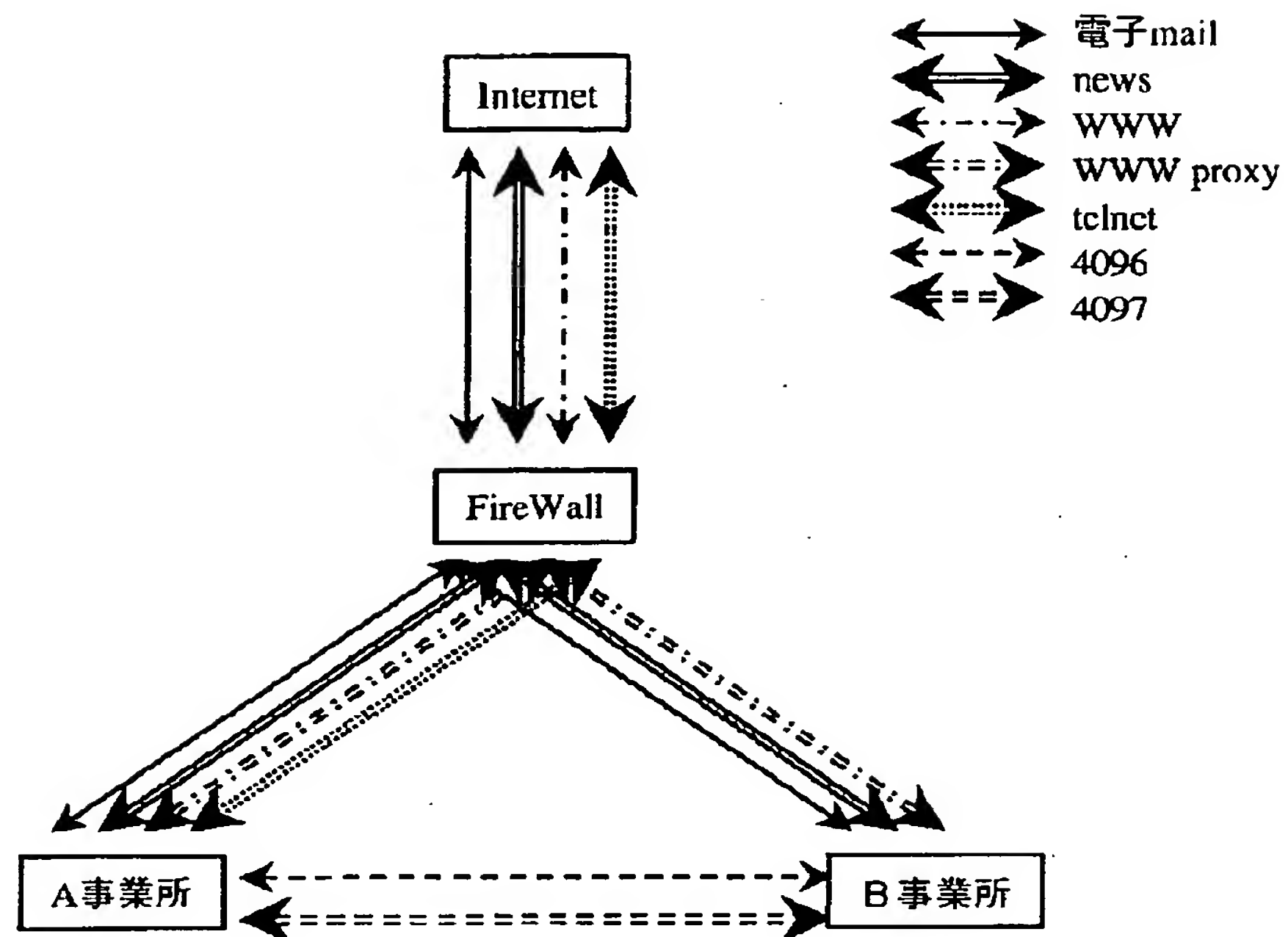
アプリケーション種別	通信先	優先度	通信禁止
電子mail	経理Zoneのみ	中	経理以外禁止
WWW proxy	経理Zoneのみ		経理以外禁止
telnet	経理Zoneのみ		経理以外禁止
5001	経理Zoneのみ	大	経理以外禁止
5002	経理Zoneのみ		経理以外禁止
5003	経理Zoneのみ		経理以外禁止

勤労Zone定義

アプリケーション種別	通信先	優先度	通信禁止
電子mail	勤労Zoneのみ	中	勤労以外禁止
WWW proxy	勤労Zoneのみ		勤労以外禁止
telnet	勤労Zoneのみ		勤労以外禁止
5101	勤労Zoneのみ		勤労以外禁止
5102	勤労Zoneのみ		勤労以外禁止
5103	勤労Zoneのみ	大	勤労以外禁止

【図4】

図4

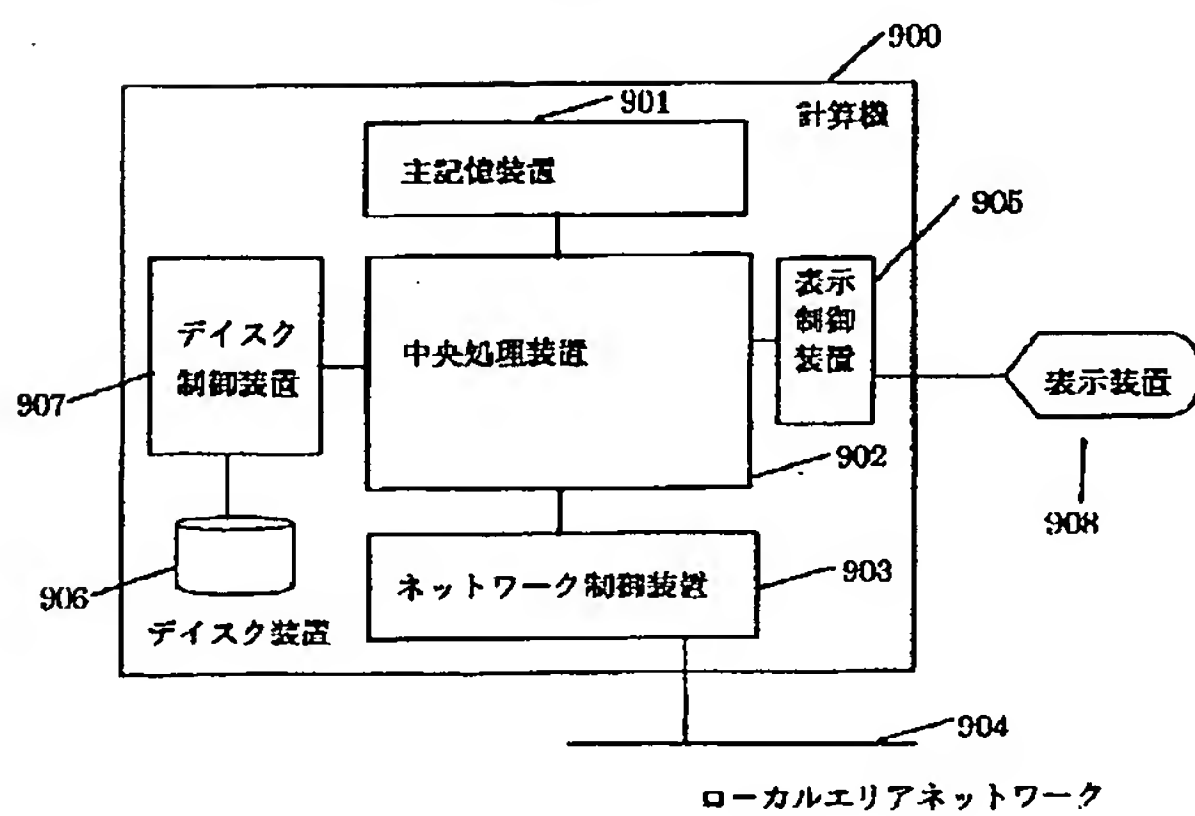


経理

勤労

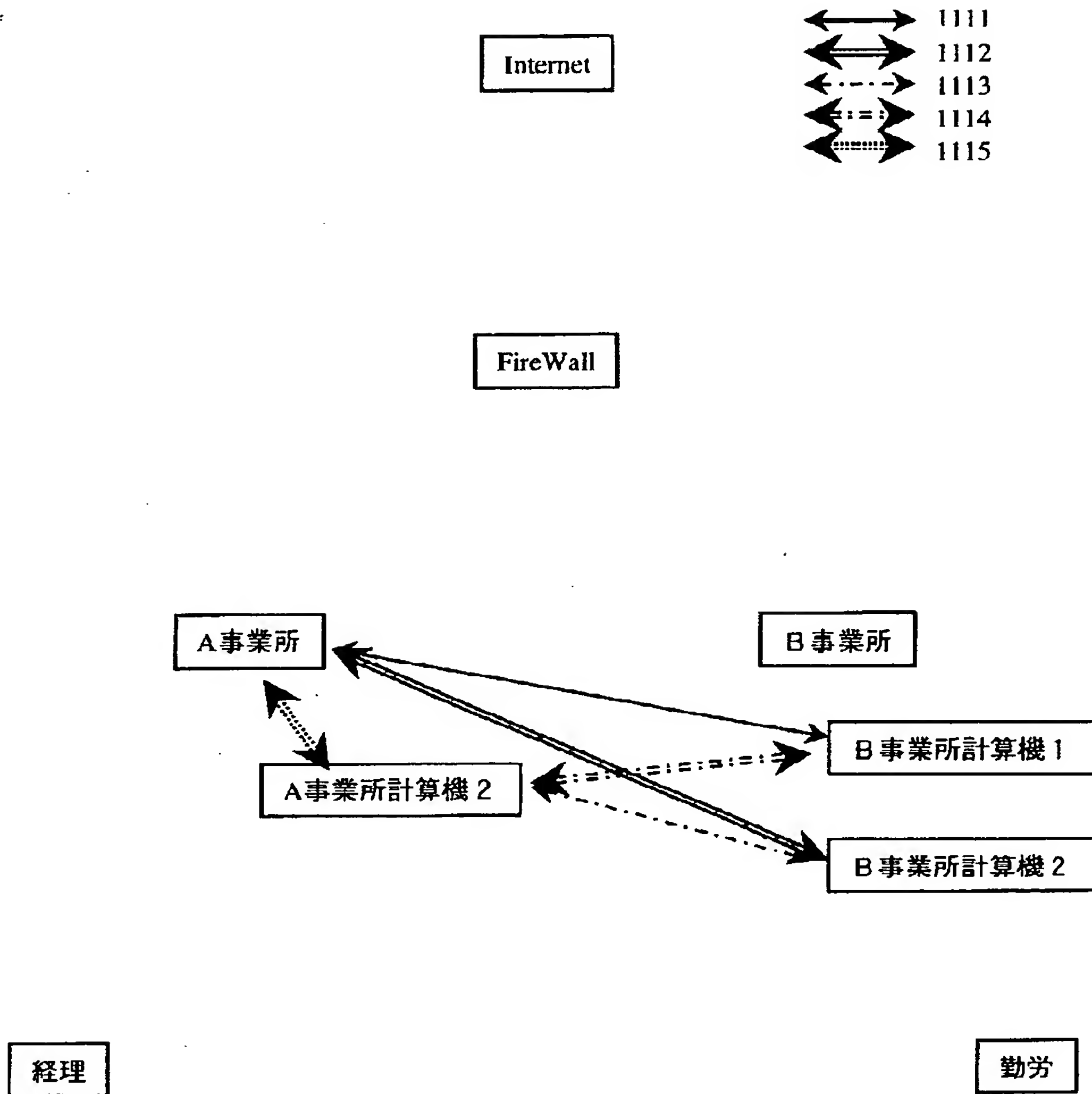
【図13】

図13



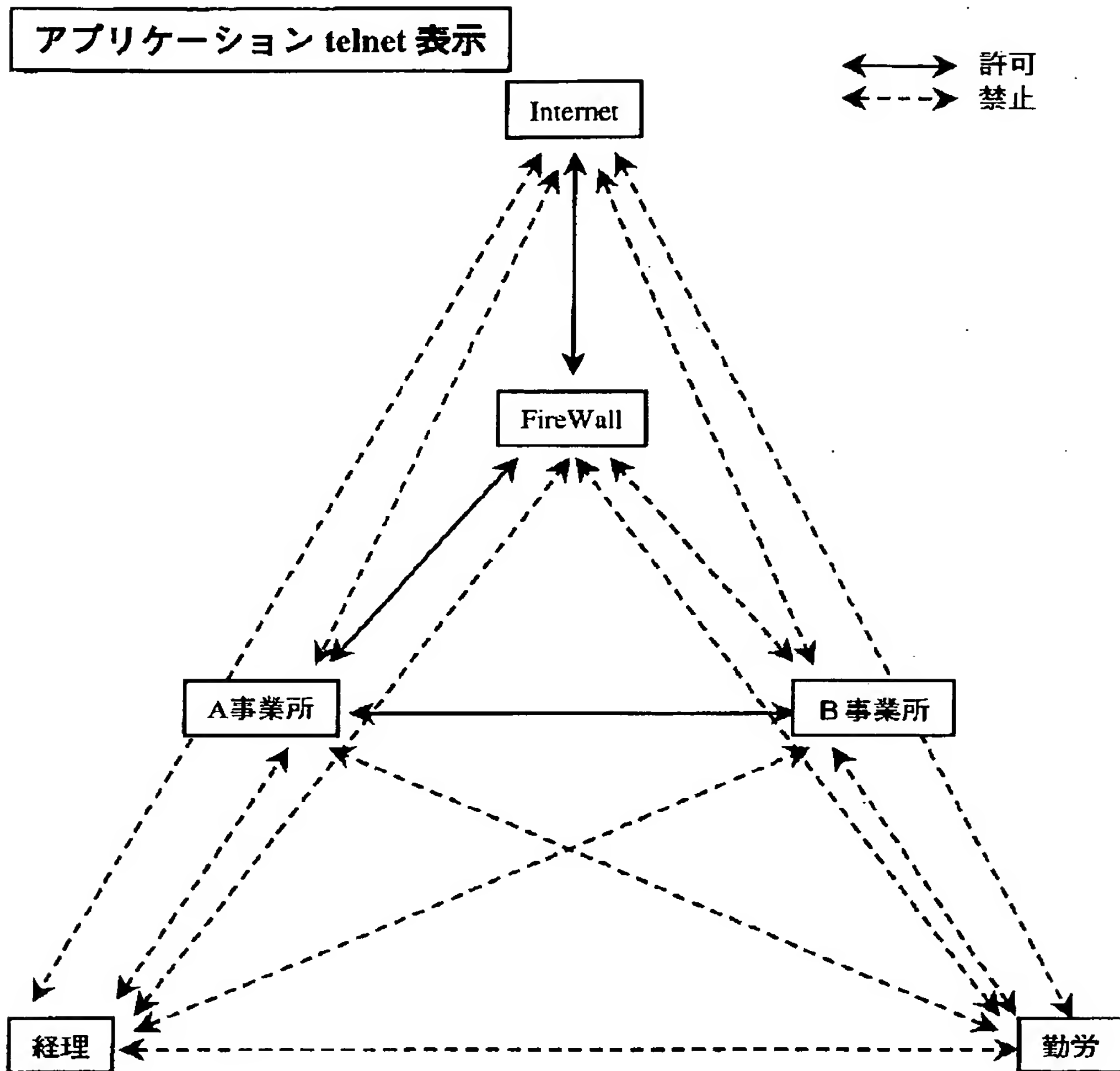
【図5】

図5



【図6】

## 図6



【図7】

図7

中間ルータ定義

設定項目	設定内容
名称	router1
ルータ初期化ファイル	X 1
FireWall Zone インターフェイス	192.10.0.1 (255.255.0.0)
A事業所Zone インターフェイス1	192.11.0.1 (255.255.0.0)
B事業所Zone インターフェイス	192.12.0.1 (255.255.0.0)
A事業所Zone インターフェイス2	192.13.0.1 (255.255.0.0)

経理VPN定義 (192.11.0.10用)

設定項目	設定内容
名称	VPN1
所属機械アドレス	192.11.0.10, 192.12.0.10
初期化ファイル	X192.11.0.10, X192.12.0.10
暗号化方式	Y1
認証方式	Y2
ポート番号	5000

【図9】

図9

中間ルータ用管理制御データ

設定項目	設定内容
名称	router1
ルータ初期化ファイル	X 1
FireWall Zone インターフェイス番号	00:20:AF:DF:87:9B
A事業所Zone インターフェイス番号1	00:20:AF:DF:87:9C
B事業所Zone インターフェイス番号	00:20:AF:DF:87:9D
A事業所Zone インターフェイス番号2	00:20:AF:DF:87:9E
制御方式	Z 1
制御用認証方式	Z 2

経理VPN用管理制御データ (192.11.0.10用)

設定項目	設定内容
名称	VPN1
インターフェイス番号	00:20:AF:DF:87:9A
初期化ファイル	X192.11.0.10
制御方式	Z 3
制御用認証方式	Z 4

【図8】

図8

A事業所関連ルータ設定 (インターフェイス1)

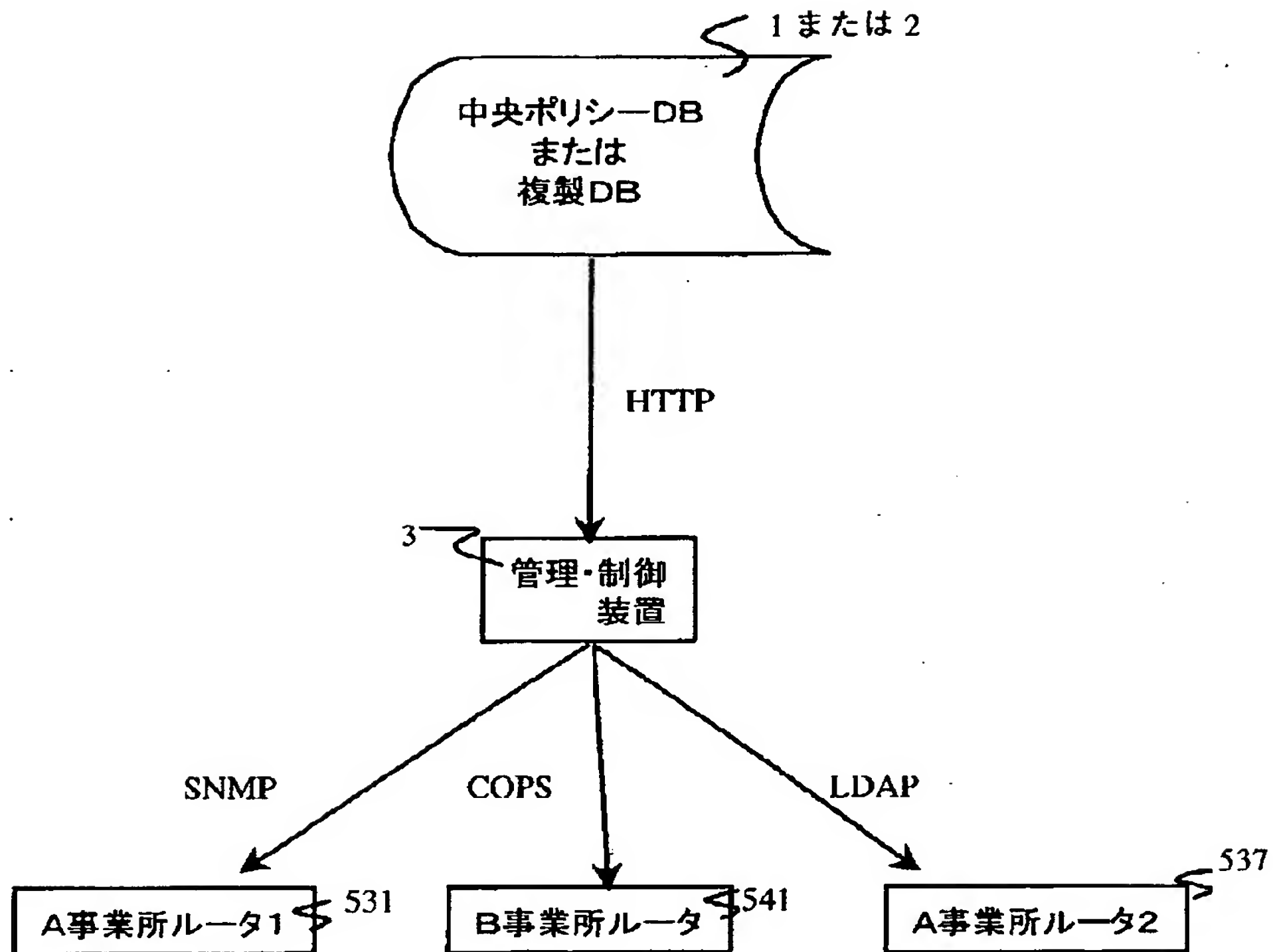
設定項目	設定内容
インターフェイスアドレス	192.11.0.1
インターフェイスマスク	255.255.0.0
アクセス許可	ポート * 番: 192.13.0.0 (255.255.0.0)
アクセス許可	ポート 1111 番: 192.12.10.1 (255.255.255.255), 優先度 2
アクセス許可	ポート 1112 番: 192.12.10.2 (255.255.255.255)
アクセス許可	ポート 1113 番: 192.12.10.2 (255.255.255.255), 192.11.10.2
アクセス許可	ポート 1114 番: 192.12.10.1 (255.255.255.255), 192.11.10.2
アクセス不許可	ポート 23 番: not 192.0.0.0 (255.0.0.0)
アクセス不許可	ポート 4096 番: not 192.0.0.0 (255.0.0.0)
アクセス不許可	ポート 4097 番: not 192.0.0.0 (255.0.0.0)
アクセス許可	ポート 5000 番: 192.12.0.0 (255.255.0.0), 優先度 0
アクセス許可	ポート 25 番: 192.10.0.0 (255.255.0.0), 優先度 2
アクセス許可	ポート 119 番: 192.10.0.0 (255.255.0.0), 優先度 1
アクセス許可	ポート 8080 番: 192.10.0.0 (255.255.0.0), 優先度 1
アクセス許可	ポート 23 番: 192.10.0.0 (255.255.0.0), 優先度 1
アクセス許可	ポート 23 番: 192.12.0.0 (255.255.0.0), 優先度 1
アクセス許可	ポート 4096 番: 192.12.0.0 (255.255.0.0), 優先度 3
アクセス許可	ポート 4097 番: 192.12.0.0 (255.255.0.0), 優先度 1
アクセス不許可	ポート * 番: 0.0.0.0 (0.0.0.0)

経理VPN設定 (192.11.0.10用)

設定項目	設定内容
暗号化方式	Y1
認証方式	Y2
通信相手アドレス	192.12.0.10 : 5000
アクセス許可	ポート 25 番: 192.12.0.0 (255.255.0.0), 優先度 2
アクセス許可	ポート 8080 番: 192.12.0.0 (255.255.0.0), 優先度 1
アクセス許可	ポート 23 番: 192.12.0.0 (255.255.0.0), 優先度 1
アクセス許可	ポート 5001 番: 192.11.0.0 (255.255.0.0), 優先度 3
アクセス許可	ポート 5002 番: 192.11.0.0 (255.255.0.0), 優先度 1
アクセス許可	ポート 5003 番: 192.11.0.0 (255.255.0.0), 優先度 1

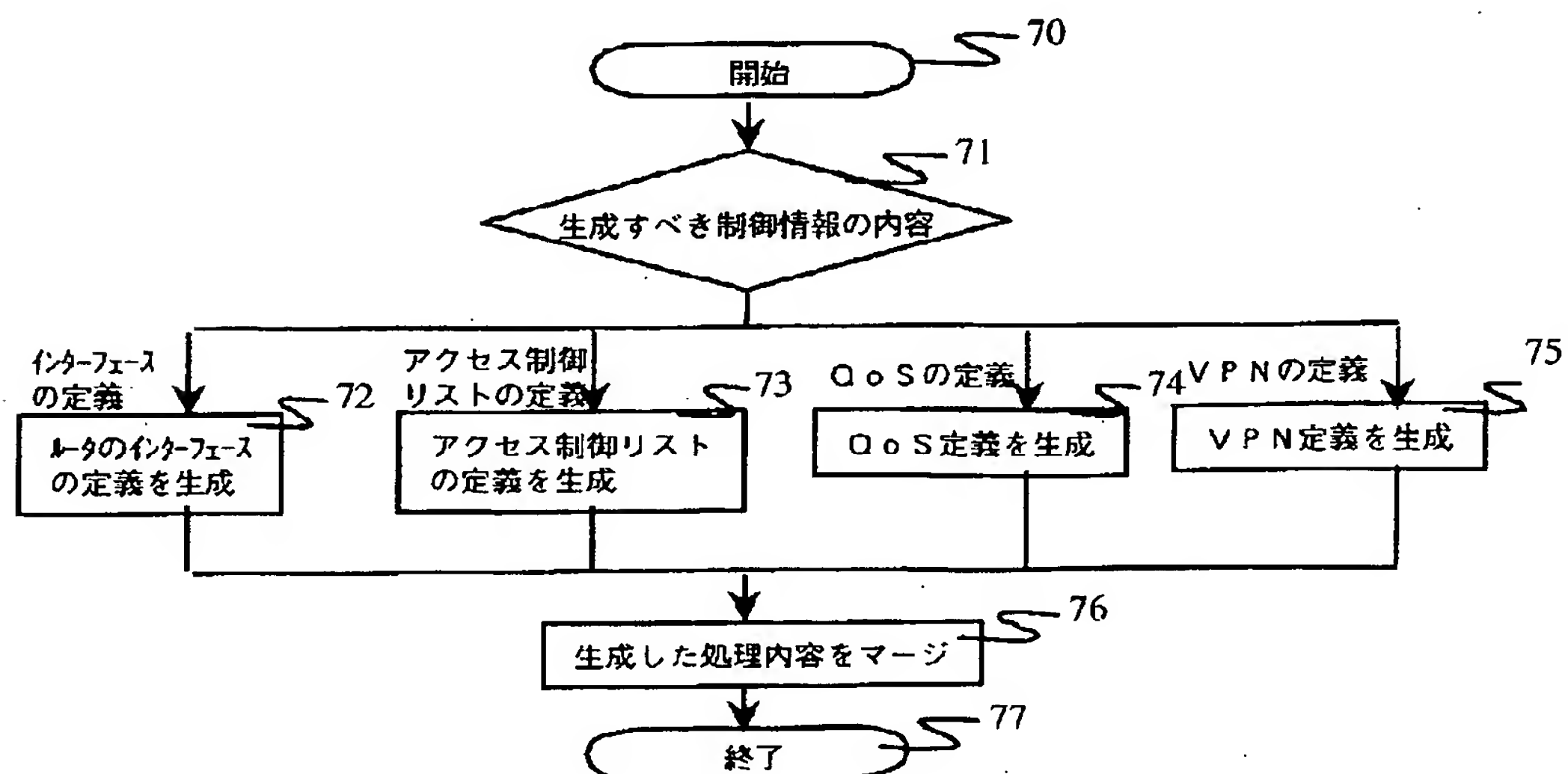
【図10】

図10

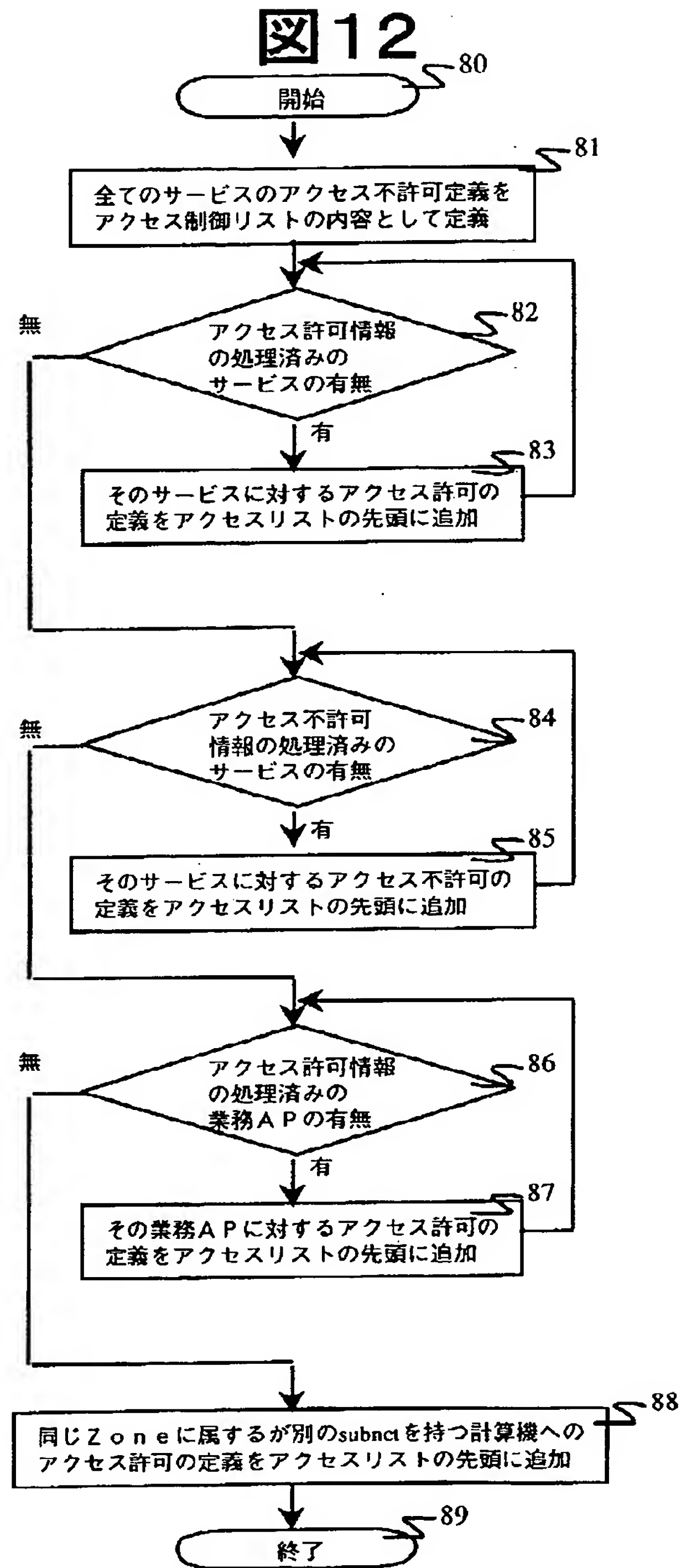


【図11】

図11



【図12】



日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出 願 年 月 日                      2 0 0 3 年 1 0 月 3 0 日  
Date of Application:

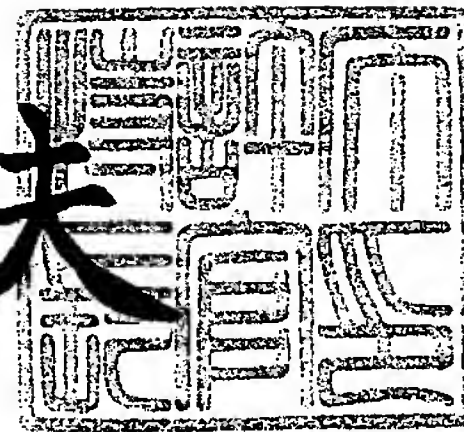
出 願 番 号                      特 願 2 0 0 3 - 3 6 9 8 1 4  
Application Number:  
ST. 10/C] :                      [ J P 2 0 0 3 - 3 6 9 8 1 4 ]

願                      人                      株式会社日立製作所  
Applicant(s):

2 0 0 3 年 1 2 月    4 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出 願 年 月 日                      2 0 0 3 年    3 月 2 0 日  
Date of Application:

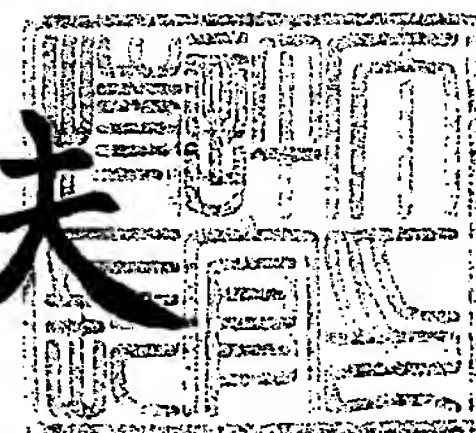
出 願 番 号                      特 願 2 0 0 3 - 0 7 9 1 6 6  
Application Number:  
[ST. 10/C] :                      [ J P 2 0 0 3 - 0 7 9 1 6 6 ]

願                      人                      株式会社日立製作所  
Applicant(s):

2 0 0 3 年 1 2 月    3 日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

今 井 康 夫



フロントページの続き

(72)発明者 平田 俊明  
神奈川県川崎市麻生区王禅寺1099番地 株  
式会社日立製作所システム開発研究所内  
(72)発明者 小泉 稔  
神奈川県川崎市麻生区王禅寺1099番地 株  
式会社日立製作所システム開発研究所内

(72)発明者 高田 治  
神奈川県川崎市麻生区王禅寺1099番地 株  
式会社日立製作所システム開発研究所内  
F ターム(参考) 5K030 GA16 HB06 HB18 HC13 HD03  
HD06 JA10 JT06 KA05 KA07  
MD07  
9A001 BB03 BB04 CC06 CC07 EE02  
EZ03 FF01 JJ02 JJ25 JJ36  
KK31 KK56 LZ03